AO 106 (Rev. 06/09) Application for a Search Warrant



# UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*
IN THE MATTER OF THE SEARCH OF THE RECORDS OF GOOGLE, INC. ASSOCIATED WITH THE EMAIL ADDRESS OF JAKE@SPECIALTYMGT.COM STORED AT PREMISES OWNED, OPERATED, MAINTAINED, OR CONTROLLED BY GOOGLE, INC., 1600 AMPHITHEATRE PARKWAY, MOUNTAIN VIEW, CALIFORNIA

Case No. 19-MJ-147-PJC

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A":

located in the Northern District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. §371 | Conspiracy to Pay Health Care Kickbacks in Violation of 42 U.S.C. § 1320a-7b(b)(2)(A) |

The application is based on these facts:

**See Affidavit of SA Shannon E. Clark, FBI, attached hereto.**

☑ Continued on the attached sheet.

☐ Delayed notice of ___ days (give exact ending date if more than 30 _____ ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Applicant's signature*

SA Shannon E. Clark, FBI
*Printed name and title*

Sworn to before me and signed in my presence.

Date: 7/19/2019

*Judge's signature*

City and state: Tulsa, OK Tulsa, Oklahoma

U.S. Magistrate Paul J. Cleary
*Printed name and title*

# AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Shannon E. Clark, being first duly sworn, hereby depose and state as follows:

## INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant to search the records of Google, Inc. (Google), a technology company specializing in Internet-related services, including electronic mail (email), storage, and communications, headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043, associated with a specific email account as further described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), to require Google to disclose to the government copies of the information and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the content of communications, as further described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been so since March 2004. I am currently assigned to the Oklahoma City Division, Tulsa Resident Agency. Prior to Tulsa, I was stationed in the FBI - Philadelphia Division. As a Special Agent with the FBI, I am charged with conducting a broad range of criminal investigations. During my tenure as a Special Agent, I have participated in training involving the execution of search warrants for documents and other evidence in cases involving violations of federal law, and have worked on numerous federal criminal investigations, including investigations of health care fraud. Through training and

participation in criminal investigations, I have become familiar with and have participated in the following methods of investigations, including, but not limited to: electronic surveillance, visual surveillance, questioning of witnesses, executions of search warrants, confidential informants and undercover agents.

3. The facts and circumstances of this investigation set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the circumstances described herein, and a review of public source information. This affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, and therefore does not include each and every fact I have learned during the course of this investigation.

4. Based on my training and experience in health care fraud, as well as other criminal investigations, and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §371 (Conspiracy to Pay Kickbacks in Violation of 42 U.S.C. § 1320a-7b(b)(2)(A)) have been committed by individuals residing in the Northern District of Oklahoma, who were subscribers to, and utilized the following Google account in the perpetuation of their fraud scheme: "jake@specialtymgt.com". There is also probable cause that the evidence of these crimes are located in the place described in Attachment A.

## JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711 and 18 U.S.C. §§ 2703(a),

(b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

## ENTITIES AND SUBJECTS

6. **OK COMPOUNDING** (OK Compounding) was an Oklahoma Limited Liability Company located in Skiatook, Oklahoma, with its business office in Tulsa, Oklahoma. OK Compounding specialized in the preparation of compounded medications. OK Compounding was licensed in Oklahoma and could fill and send prescriptions to Oklahoma residents.

7. **ONE STOP RX** (One Stop) was an Oklahoma Limited Liability Company located in Tulsa, Oklahoma, that was controlled by Christopher R. Parks. One Stop was a licensed pharmacy that dispensed both compounded and non-compounded medications.

8. **CHRISTOPHER R. PARKS** (Parks) was part owner of OK Compounding. Parks and Gary Robert Lee controlled One Stop and Specialty Pharmacy Management. Parks solicited prescriptions that yielded high reimbursements through financial relationships with doctors, both directly and through third-party marketing groups.

9. **SPECIALTY PHARMACY MANAGEMENT** was an entity established by Parks to facilitate the payment of kickbacks to doctors and marketers, in exchange for referring prescriptions to OK Compounding or One Stop RX.

10. **JAKE GROSVENOR** was the Financial Coordinator for OK Compounding and Specialty Pharmacy Management.

11. **USA HEALTHCARE** was a marketing company responsible for referring TRICARE prescriptions to OK Compounding and One Stop RX. They received payments from Specialty Pharmacy Management.

12. **NOAH SILVERMAN** was one of the managers of USA Healthcare.

## TRICARE

13. TRICARE provided health care coverage for Department of Defense (DOD) beneficiaries world-wide, including active duty service members, National Guard and Reserve members, retirees, their families, and survivors.

14. Individuals who received health care benefits through TRICARE were referred to as TRICARE "beneficiaries." The Defense Health Agency ("DHA"), an agency of the DOD, was the military entity responsible for overseeing and administering the TRICARE program.

15. TRICARE provided coverage for certain prescription drugs, including certain compounded drugs, if the drugs were medically necessary and prescribed by a licensed physician. Express Scripts is the company that administered the TRICARE prescription program. If a beneficiary chose a network pharmacy, the pharmacy would collect any applicable co-pay from the beneficiary, dispense the drug to the beneficiary, and submit a claim for reimbursement to Express Scripts, which would in turn adjudicate the claim and reimburse the pharmacy. To become a TRICARE network pharmacy, a pharmacy agreed to be bound by, and comply with, all applicable State and Federal laws, specifically including those addressing fraud, waste, and abuse.

16. OK Compounding and One Stop, through Pharmacy Providers of Oklahoma (PPOK), submitted claims and received reimbursement for prescription compounding drugs it dispensed to TRICARE beneficiaries.

17. TRICARE was at all relevant times a "Federal health care program," ("Federal") as defined by 42 U.S.C. § 1320a-7b(f), that affected commerce.

**PHARMACY MANAGEMENT**

18. On March 27 and 28, 2019, an interview of Noah Silverman was conducted regarding his involvement with soliciting prescriptions for Parks' enterprises and receiving payment for the same.

19. Silverman explained that between 2013 and 2015, a company managed by Silverman, USA Healthcare, operated a call center that generated prescriptions for Parks' pharmacies. The call center utilized leads to identify patients potentially interested in receiving compounded medications. When the phone operator contacted the patient, they would inquire as to whether or not the patient was interested in receiving compounded medications. If the patient responded in the affirmative, the call center would transfer the patient call to a telemedicine doctor, who would write a prescription for medication that was then sent to one of Parks' pharmacies to fill.

20. The compensation agreement that Silverman entered into with Parks was a commission-based system wherein USA Healthcare was paid a percentage of profits derived from prescriptions they sourced for Parks' pharmacies.

21. These prescriptions included payments on prescriptions reimbursed by TRICARE.

22. A federal search warrant was executed on October 9, 2014 on OK Compounding and Specialty Pharmacy Management.

23. After the federal search warrants, Silverman was contacted by Parks. Parks advised him that the compensation arrangement needed to be changed. Rather than going from a straight commission payment, the monthly commission paid to USA Healthcare would be calculated under the previous terms of business, but an intermediate step would be added.

24. Rather than a commission payment be remitted directly to USA Healthcare, the dollar amount of the commission would be "reverse-engineered" into an invoice billing for hours of services rendered to Parks' entities by USA Healthcare.

25. Silverman advised that the revised payment scheme was implemented on December 1, 2014.

26. According to Silverman, disputes over the amount of commission owed to USA Healthcare from Parks resulted in draft versions of the billing invoice, but ultimately, the payment from Parks to USA Healthcare was backstopped by a billing invoice for labor hours that matched the amount owed USA Healthcare under their original commission arrangement with Parks.

27. To illustrate the process, Silverman produced an email sent to him from Grosvenor. The email, dated May 13, 2015, read in relevant part:

*Brooke,*

*Due to returns we need you to adjust your invoice to recoup some of the costs of these returns.*

*Please make allowance of $16,000. If you have any questions please let Christopher know.*

28. On May 21, 2019, your affiant participated in an interview of Grosvenor.

29. During the interview, Grosvenor stated that after the search warrants executed by your affiant on OK Compounding and Specialty Pharmacy Management in October 2014, Parks authorized "hourly payments" in order to hide commission payments for prescriptions from federal health care programs. Grosvenor stated it was common practice for Parks entities to "reverse-engineer" commission payments for federal health care programs into invoices for hours worked.

30. Grosvenor added that at the time of his departure from the company (a few weeks prior to the May 21, 2019 interview), he was aware of at least 30 consultants being paid in this manner.

31. Grosvenor stated that all draft and final invoices were contained in his work email (jake@specialtymgt.com).

## BACKGROUND CONCERNING EMAIL

32. Your affiant was the affiant for search warrants that were executed on OK Compounding and Specialty Pharmacy Management in October 2014. Additionally, multiple Grand Jury subpoenas have been issued to Parks' Entities and business associates of Parks' Entities.

33. The material obtained from prior subpoenas and search warrants of OK Compounding and Specialty Pharmacy management in October 2014 contained emails, including emails authored by Grosvenor.

34. Review of the emails indicated that Grosvenor's work email for a significant duration of the conspiracy was jake@specialtymgt.com. Review of records obtained by the government supported that this email address was used by Grosvenor to discuss commission payments to marketers.

35. On January 13, 2015, an email was sent from jake@specialtymgt.com to Noah Silverman at noah@rxpharmacynetwork.com that reads, in relevant part:

*HOANG TOTAL $ 374,927.41*

*HOANG PAID $ 347,000.00*

*ALL OTHER DOCS $ 28,661.48*

*45% $ 12,897.67*

*OWE $ 12,897.67*

*Noah, a wire was sent for this amount today. See breakdown attached.*

This email appears to be feedback about the amount of money USA Healthcare could expect from Specialty Pharmacy Management, consistent with the statements of Silverman and Grosvenor.

36. Your affiant further reviewed an email obtained under grand jury subpoena regarding the email service provider utilized by Specialty Pharmacy Management. The email was sent on November 11, 2014 by Linda Floyd, an employee of Specialty Pharmacy Management, and received by multiple employees and email users of Specialty Pharmacy Management, including Grosvenor. The email reads, in relevant part:

*Team,*

*We have officially switched our email service from Godaddy to Gmail!*

*You will now access your email at http://mail.google.com. Username is your specialty email address and password is specialtymgt.*

*After you login for the first time, you will need to change your password.[...]*

37. On May 30, 2019, the email address jake@specialtymgt.com was tested through a multi-level, server side, bad address filter. The test determined that as of that date, the domain @specialtymgt.com existed, and that the email server associated with it did not reject jake@specialtymgt.com as a bad email address. The same test identified the Mail Exchange (MX) servers hosting the email as Google servers.

## BACKGROUND CONCERNING EMAIL PROVIDER

38. In general, an email that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

39. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at both the domain name @gmail.com, as well personalized domain names for business accounts such as @specialtymgt.com, like the email accounts listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and

information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

40. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

41. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP

addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

42. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

43. This application seeks a warrant to search all responsive records and information under the control of Google, a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

44. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each

element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

## CONCLUSION

45. Based on the aforementioned facts and circumstances, Affiant believes there is probable cause that information maintained by Google on email account jake@specialtymgt.com contains evidence, fruits, and or instrumentalities of violations of statutes as previously noted. I therefore respectfully request this Court to issue a search warrant for the location listed in Attachment A and the items listed in Attachment B.

46. Due to the fact Google, upon receipt of this warrant, will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time, day or night. Additionally, pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

## REQUEST FOR SEALING

47. Affiant further requests the Court order all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents as premature disclosure may give targets an opportunity to flee from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

SA Shannon E. Clark, FBI

Subscribed and sworn to before me on July 19, 2019.

PAUL J. CLEARY
United States Magistrate Judge

## ATTACHMENT A

### Property to Be Searched

The property to be searched is all records of Google, Inc., wherever stored, associated with the Google email, storage, and communication accounts known as:

- jake@specialtymgt.com

that are stored at premises owned, maintained, controlled, or operated by Google Incorporated, a company headquartered at 1600 Amphitheater Parkway, Mountain View, California 94043.

# ATTACHMENT B

## Particular Things to be Seized

### I. Information to be disclosed by Google, Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails and attachments associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

## II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §371 (Conspiracy to Pay Kickbacks in Violation of 42 U.S.C. § 1320a-7b(b)(2)(A), those violations involving the user(s) of "jake@specialtymgt.com" and others known and unknown, and occurring between **January 1, 2014, and Present.**

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.